IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal Action No. 1:17-CR-302
	)	
NIKOLAI BOSYK,	)	Honorable Leonie M. Brinkema
	)	
Defendant.	)	Motions Hearing: February 2, 2018
	)	Trial: February 19, 2018

UNITED STATES' RESPONSE TO
DEFENDANT'S MOTION TO SUPPRESS

The United States of America, through undersigned counsel, respectfully submits this memorandum of law setting forth the reasons why the defendant's pending motion to suppress the fruits of the April 12, 2016, search of his residence should be denied.

PRELIMINARY STATEMENT

Nikolai Bosyk downloaded and possessed thousands of videos and images containing child pornography. He acquired this content by visiting websites that catered specifically to individuals interested in obtaining content featuring young boys and girls being sexually abused. One of the websites that he visited was Bulletin Board A, which was only accessible on the dark web via a special web-browser called TOR.[1] Bulletin Board A advertised child pornography content for child sexual predators organized in a traditional internet message-board format. On Bulletin Board A, users posted links to child pornography which, when clicked, led to a webpage where the child pornography file could be downloaded. Because the webpage storing the child pornography was

[1] TOR is a network designed to facilitate anonymous communication. One aspect of TOR is the ability for users to set up websites—like Bulletin Board A—that are accessible only to users operating within TOR.

not hosted on TOR, when a user clicked the link there to initiate the download of a file, that website recorded the user's IP address. Defendant's internet protocol (IP) address was captured as having initiated such a download. Specifically, a URL linking to child pornography was posted on Bulletin Board A on November 2, 2015. That same day, November 2, 2015, someone at the defendant's residence clicked on that link to initiate downloading the child pornography. Law enforcement traced that IP address to a residence in Purcellville, Virginia – a residence where Nikolai Bosyk lived.

The click of the link that law enforcement identified on Bulletin Board A, the recording of the IP address of the computer that accessed that link, and the information connecting the defendant's residential address with that IP address provided sufficient basis for investigators to believe and United States Magistrate Judge Michael S. Nachmanoff to conclude that evidence of child pornography would be at the premises. That is why a search warrant was issued.

Despite this simple set of facts, the defendant seeks to suppress all of the incriminating evidence found at his residence. The overwhelming body of case law in this circuit stands firmly against suppression. Yet, the defendant, relying on inapposite cases from the Second Circuit and a single district court case from Norfolk, asks this court to grant the extraordinary remedy of exclusion. This court should refuse to do so.

ARGUMENT

Probable cause existed to search the defendant's home on April 12, 2016, because law enforcement determined that a computer at the defendant's residence accessed a link containing child pornography, which originated on a website that caters to individuals seeking child pornography. The search warrant issued based on these facts was facially valid. The defendant now seeks to suppress the evidence seized by agents during the search, arguing: (1) that probable

cause was lacking to issue the warrant; and (2) that even if there was probable cause initially, by the time the agents executed the warrant, it was based on stale information. The defendant also argues that an evidentiary hearing pursuant to *Delaware* v. *Franks* is appropriate and that if it is determined that the warrant is invalid, the good faith exception is inapplicable.

As will be discussed below, the overwhelming weight of the case law supports existence of probable cause here because the magistrate could have concluded that there was a "fair probability" that evidence of child pornography would have been located at the defendant's residence. *Illinois* v. *Gates*, 462 U.S. 213, 238-39 (1983). There is likewise no staleness defect here because courts in this circuit and around the country acknowledge that individuals who possess child pornography tend to keep their material for long periods. *United States* v. *Richardson*, 607 F.3d 357, 370 (4th Cir. 2010); *see also United States* v. *Harvey*, 2 F.3d 1318, 1323 (3d. Cir. 1993) (holding that 15-month old information is not stale in child pornography context).

Furthermore, a *Franks* hearing in this case is inappropriate because the defendant cannot make the proper showing of agent misconduct or recklessness as required by the law. *See United States* v. *Clenney*, 631 F.3d 658, 663 (4th Cir. 2011) (outlining the rigorous standard applicable to make a showing for a *Franks* hearing). Finally, because law enforcement relied on the probable cause determination of the magistrate judge to conduct the search, the good faith exception applies. *United States* v. *Leon*, 468 U.S. 897, 922 (1984).

I. THERE IS NO BASIS TO EXCLUDE EVIDENCE FROM THE SEARCH OF THE DEFENDANT'S RESIDENCE.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures" and instructs that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

describing the place to be searched, and the person or things to be seized." U.S. Const. Amend IV. To prevent the abuse of the Fourth Amendments protections, courts have instituted an "exclusionary rule" to prevent evidence obtained during an illegal search from being used at trial. *United States* v. *Kimble*, 855 F.3d 604, 610 (4th Cir. 2017).

While the exclusionary rule is available to suppress items from illegal searches, the Supreme Court has cautioned that suppression of evidence is "our last resort, not our first impulse." *Hudson* v. *Michigan*, 547 U.S. 586, 591 (2006). It has noted the "substantial social costs" from use of the exclusionary rule, *United States* v. *Leon*, 468 U.S. 897 (1984), including "the loss of often probative evidence and all of the secondary costs that flow from the less accurate or more cumbersome adjudication that therefore occurs." *INS* v. *Lopez-Mendoza*, 468 U.S. 1032, 1041 (1984). Because of those social costs, courts are reluctant to apply the exclusionary rule. And as a result, "the exclusionary rule is not a remedy . . . appl[ied] lightly." *Sanchez-Llamas* v. *Oregon*, 548 U.S. 331, 347 (2006). Given this body of law, here, where there is probable cause and no police misconduct, suppression is unwarranted.

A. PROBABLE CAUSE EXISTED FOR THE ISSUANCE OF THE SEARCH WARRANT BECAUSE THERE WAS A FAIR PROBABILITY THAT CHILD PORNOGRAPHY WOULD BE LOCATED AT THE DEFENDANT'S RESIDENCE.

The information in the affidavit provides ample information supporting probable cause. The affidavit: (1) identifies the existence of a website, which caters specifically to a community of users looking to trade child pornography; (2) identifies a specific post in a sub-forum catering to pre-teen hardcore content, which on its face provides thumbnails of child pornography and a link to download that child pornography; and (3) provides information demonstrating that a computer with an IP address that can be traced back to the defendant's residence attempted to download the child pornography the same day it was posted on that website. Essentially, as the

law required, this information linked criminal activity—downloading or attempting to download child pornography—to the place to be searched, and provided Judge Michael Nachmanoff (the issuing magistrate) with a reasonable basis to conclude that there was a "fair probability" that contraband would be located at the residence.

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas* v. *United States*, 517 U.S. 690, 696 (1996). A magistrate judge conducts the assessment and decides whether there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois* v. *Gates*, 462 U.S. 213, 238–39 (1983). This assessment is "a practical, common-sense decision, given all the circumstances set forth in the affidavit." *Id.* at 238.

Importantly, the test for a search warrant is not whether the affidavit links a particular person to a crime, but rather "whether it is reasonable to believe that the items to be seized will be found in the place to be searched." *United States* v. *Lalor*, 996 F.2d 1578, 1582 (4th Cir. 1993). This emphasis on the place to be searched is crucial. As the Fourth Circuit has held, all that is required is that the "[i]nformation must link criminal activity to the place to be searched." *United States* v. *Testerman*, 263 F. App'x 328, 330 (4th Cir. 2008).

Applying these principles, the affidavit in support of the search warrant in this case contains ample information that links criminal activity at the defendant's residence. The link to download child pornography that led investigators to the defendant's residence was discovered on Bulletin Board A. The affidavit describes Bulletin Board A as "an internet-based bulletin board dedicated to the advertisement, distribution and production of child pornography." Affidavit at ¶ 5. The affidavit notes that Bulletin Board A "has various sections containing forums and sub forums in

which members post messages or images for other members", including sections labeled "Pre-teen Hardcore, Pre-teen Softcore/Non-nude, Teen/Jailbait, . . . Babies and toddlers, and Requests." *Id.* at ¶ 6. This information establishes that Bulletin Board A is a place that actively caters to individuals seeking to acquire or share content depicting child sexual abuse.

Next, the affidavit details a law enforcement investigation into Bulletin Board A. This investigation, which began in October 2015, sought to identify individuals responsible for distributing and acquiring child pornography on Bulletin Board A. During the course of the investigation, law enforcement identified a post by a board member in the "Pre-teen Hardcore, sub forum Videos" which indicated that the board member was sharing "4 small clips of beautify pussy and ass, some include finger inserting . . . Hope all of you enjoy my videos." *Id.* at 7. As Special Agent Eyler then noted in her affidavit, "[b]elow the posts are twenty video thumbnail images that depict an adult male using his fingers to spread the vagina of a female who appears to be a toddler." *Id.* Importantly, to download this content via a link provided in the post, a user had to enter a password, which was provided in the body of the post. *Id.* at 8.

The affidavit then provides the magistrate with some background on the File Sharing Site, or FSS, which hosted the file being distributed on Bulletin Board A. *Id.* at ¶¶ 11–13. Because it did not operate on TOR like Bulletin Board A, FSS was able to log the IP addresses which attempted to access the file linked on Bulletin Board A, and law enforcement was able to compel disclosure of those IP addresses using legal process. One of the IP addresses that attempted to download the known child pornography file was 208.89.176.122, which traced back to the defendant's residence. *See id* at. ¶¶ 16–18.

Despite the clear link between the illegal activity and the place to be searched, the defendant seeks suppression of the significant body of incriminating and illegal materials in his

possession at the time the search was executed. To convince this court to compel suppression, the defendant makes three main arguments to undermine probable cause. First, the defendant argues that the "affidavit fails to allege Mr. Bosyk clicked on any link in Bulletin Board A or that Bulletin Board A was the means that his IP address attempted to access the subject URL." Def. Mot. to Suppress at 4. Second, the defendant complains that "there is no evidence or accusation that the actual content, alleged to contain child pornography was ever accessed, viewed, downloaded, or otherwise utilized . . . by Mr. Bosyk." *Id.* Third, Mr. Bosyk protests that nothing in the affidavit connects him to being a collector of child pornography. *Id.* at 5. None of these arguments have merit.

1. The affidavit does not allege that Mr. Bosyk clicked on any link in Bulletin Board A because there was no evidence at the time that the defendant was the individual who clicked on the link at Bulletin Board A. The evidence acquired only showed that a computer that traced back to the defendant's residence was responsible for accessing or attempting to access the child pornography which was distributed at Bulletin Board A. Indeed, the very purpose of the warrant was to continue the investigation to determine who, specifically, attempted to access the child pornography at Bulleting Board A. Without the aid of a search warrant to allow seizure of the electronic devices at the residence (and subsequent forensic analysis), it would be difficult for law enforcement to determine with precision who accessed the child pornography at Bulletin Board A.

2. Similar to the reason that the affidavit did not contain allegation that Mr. Bosyk clicked on the link at Bulletin Board it, the affidavit also avoids alleging that Mr. Bosyk viewed, accessed, or downloaded the child pornography from Bulletin Board A. Again, the focus of the search warrant was the link between the illegal activity and *the place to be searched*. This is in essence the difference between an affidavit for a search warrant and an affidavit for a criminal complaint,

which necessarily contains allegations linking a particular *defendant* to criminal activity. *Compare* Doc. No. 2 (Affidavit in Support of a Criminal Complaint) with Affidavit in Support of Search Warrant.

3. Finally, the defendant argues that the collector language in the affidavit (*see* ¶¶ 21 – 23) is not appropriate. The collector language was included because the link to child pornography was found on a website that catered to those who shared and distributed child pornography. The collector language was not based merely on a single click to download child pornography as the defendant claims. The use of the collector language in these circumstances is appropriate.

The defendant relies chiefly on a case from this district, *United States* v. *Reece*, 2:14-cr-104, Doc. No. 44 (E.D. Va. March 1, 2017), to support his arguments. Respectfully, this Court should decline to follow the reasoning in *Reece.* In *Reece*, the court determined there was insufficient probable cause to support the search warrant in a Bulletin Board A case. The court first considered that the affidavit did not demonstrate that the defendant's IP address had ever accessed Bulletin Board A. *Id.* at 10–11. The court was concerned because it was "*possible* that the link could have been accessed through innocent means." *Id.* at 11 (emphasis added). The court also determined that there was no evidence to support the inclusion of "collector language" in the affidavit. *Id.* at 11–14.

However, the *Reece* court's findings misinterpret the standard for probable cause. The mere possibility that the child pornography could have been accessed through innocent means does not mean there is not a fair probability that it was accessed through Bulletin Board A. *See United States v. Gary*, 528 F.3d 324 (4th Cir. 2008) (finding that the mere possibility that trash cans in which contraband was found may have belonged to someone other than defendant did not defeat probable cause). This is particularly true given 1) there was no reason for the agent to believe the

link was available anywhere other than on Bulletin Board A and 2) defendant's IP address attempted to download the file in question *the same day* the link was posted on Bulletin Board A. The court's order in *Reece*—where the time between posting and download was only two days—does not consider this important point.

These facts, however, establish a fair probability that the link was accessed through Bulletin Board A and do not require a great inferential leap as defendant suggests. It is unlikely the URL was accessed somewhere else given the close proximity in time between the posting at Bulletin Board A and attempt to download its child pornographic content. That is precisely what another court considering the very same issue and the same relevant facts concluded. *United States* v. *Evans*, 2:16-cr-20292, Doc. No. 69, report and recommendation, at 14 (E.D. Mich. Nov. 20, 2017) (noting that while it is possible that the Defendant arrived at the URL by mistake, "the existence of the possibility of mistake does not negate the fair probability that child pornography will be found on a computer at the IP address's registered residential address when that IP address was used to access, download, and/or attempted to download file content associated with the URL/video at issue that was posted, at the most, 25 hours before."), *report and recommendation adopted at* Doc No. 75.

These same facts support the inclusion of collector language. A fair probability that the IP address in question accessed the child-pornography file through Bulletin Board A in turn establishes a fair probability that the person accessing the file is a collector, given Bulletin Board A's dedication to child pornography and the steps it takes to access a site like Bulletin Board A that is hosted on TOR.

In support of its decision, the court in *Reece* relies on two cases from the Second Circuit. The first case, *United States* v. *Falso*, 544 F.3d 110 (2d Cir. 2008), considered the question of

whether probable cause existed to search the defendant's home based on the allegation that the defendant "appears to have gained or attempted to gain access to a site that contained approximately eleven images of child pornography." *Id.* at 113. The defendant in *Falso* argued that suppression was necessary because there was no allegation that he was a member of the website containing child pornography. The Second Circuit, in a divided panel, held that probable cause was lacking because "there is no allegation that [the defendant] gained access" to the website and that there were no allegations "that the sole or principal purpose of the [website] was the viewing and sharing of child pornography, much less that images of child pornography were downloaded from the site." *Id.* at 124.

But *Reece's* reliance on *Falso* is misplaced. The Second Circuit stressed that while membership or subscription to a child pornography website is instructive based on its earlier precedent, "nothing in [those precedents] should be read to require these conditions in all similar cases." *Id.* at 120. It went on to note specifically that "the absence of membership would not be dispositive if other factors – such as evidence that the defendant otherwise downloaded illegal images – were present." *Id.*

This case presents precisely the type of "other factors" that the court in *Falso* stressed. Here, someone at the defendant's residence downloaded or attempted to download child pornography. Unlike in *Falso*, the probable cause here is not the mere fact that the defendant accessed the website distributing child pornography. The probable cause here is based on the fact that someone in the defendant's residence downloaded or attempted to download child pornography from a link located in a post at Bulletin Board A. *Falso* is, therefore, inapposite.

The other case from the Second Circuit that both the court in *Reece* and the defendant rely upon is *United States* v. *Coreas*, 419 F.3d 151 (2d Cir. 2005). The facts and circumstances

surrounding the suppression in *Coreas* are even less analogous to the instant case than those in *Falso*. In *Coreas*, the defendant became a member of an e-group that catered to content featuring kids and distributed content via email. Members could elect to receive each individual email from the group members, a daily digest of all the groups' emails from that day, or could elect not to receive emails from the group at all.

The court in *Coreas* found that an FBI agent made several factual assertions in a search-warrant affidavit that were knowingly or recklessly false. For example, the agent indicated that in order to join the e-group, members had to send an email message to the group's moderator. That was not true. The agent also indicated that all members of the group had to elect to either receive all the email messages either individually or as part of the digest (even though members could instead elect to refuse to receive emails).

The defendant in *Coreas* was subject to a search of his home based on an affidavit that included some of these false assertions. In particular, the affidavit claimed that the defendant had received hundreds of images and videos of child pornography. In reality, the government "had no knowledge of what Coreas had received - - even though, as subsequently determined, this was information it could have readily obtained from [email service provider] if it had sought to do so." *Id.* at 153. The Court concluded that "[a]ll that [the defendant] did, so far as the excised affidavit shows, was to respond to a three-sentence suggestive invitation from the [group] to join its e-group by clicking a button that added his e-mail address to its roll of members, but in no way committed him to partaking in any of its various activities, lawful or unlawful." *Id.* at 156.

The defendant here seizes on the "click of a button" language in *Coreas* to claim that "the single click on a URL, in and of itself, is utterly insufficient as a matter of law to establish probable cause." Def's Mot. to Suppress at 10. While merely joining an e-group without evidence that an

individual either attempted to or did acquire illicit material falls short of the Fourth Amendment's requirements, a click of a URL that was advertising child pornography on a website dedicated to child pornography does establish probable cause that evidence of that child pornography will be found at the residence where the click originated.

Further distinguishing this case from *Coreas* is the fact that while merely joining an e-group is not illegal, downloading child pornography (even a single image) is. *See* 18 U.S.C. 2252(a)(2). In this case, the single click of a button allowed the defendant to download *four* images of child pornography. This court should resist the temptation to simplify the Fourth Amendment's standard of law to fit rigid clichés like of "clicks of a button." Clicks of a button in today's interconnected world can cause significant havoc and result in significant consequences.

Despite this shortcoming, the Second Circuit's decision in *Coreas* is instructive in one respect. It noted that the government had the ability to conduct a search of the defendant's email account to determine if the defendant had received illegal contraband. *Id.* at 156 (noting the Court could have searched the defendant's Yahoo email account to determine if the defendant had received content with child pornography). Reading the decision this way, the language in *Coreas* supports the validity of the search warrant here. What led to the suppression in *Coreas* (aside from the misstatements of the agent) was not that there was an attempted search based on the facts in the affidavit, but that the search was of the wrong *place*. Had the same affidavit been for a search of email – where the agents could determine whether contraband was actually received by the defendant – the court suggests that such a warrant would have been valid. *Id.* Here, by contrast, the search warrant was for precisely the place where the investigation determined the child pornography was most likely to be: Bosyk's residence.

Next, the defendant claims that the URL at issue in the search warrant is identified differently in separate places in the affidavit, and the affidavit therefore fails to connect defendant's IP address to a child-pornography file. *See* Def's Mot. to Suppress at 3 ("The affidavit does not match the subject unique URLs outlined in para. 7 through 8 and para 16."). This is not so. As the affidavit makes clear, the URL in paragraph 16 is the same as the one referenced in paragraphs 7 and 8. *See* Affidavit at ¶ 16 ("On November 2, 2015 at 15:23:16 hours IP address 208.89.176.122 was used to download or attempt to download file content associated with that URL, which *as detailed above*, consisted of four child pornography videos.") (emphasis added). The only difference between the URL identified in paragraph 8 and paragraph 16 of the affidavit is that the agent redacted more of the file name in paragraph 8 than she did in paragraph 16. Such a minor difference, particularly when viewed in the context of affidavit, which indicates that the two URLs are the same in substance, does not defeat probable cause.[2]

Finally, the defendant asserts that there is no allegation that the defendant entered the password in order to download the child pornography. Def's Mot. to Suppress at 5. But there's no need to include this information (nor was there any way for law enforcement to determine whether Bosyk did so absent the search and forensic analysis of his computer). The fact that the link was clicked by a computer at the defendant's residence, *see* affidavit at ¶¶ 16-19, and the password was available in the post containing the link, *see* affidavit at ¶¶ 7-8, establishes a fair probability that whoever clicked that link accessed the child pornography.

[2] The link in paragraph 16 of the affidavit is slightly different from the actual link that appeared on Bulletin Board A. This was a typographical mistake, however, rather than a substantive error. The URL as spelled in the affidavit is http://[redacted].comxu5me9erdipp/brochure.rar.html. The link on Bulletin Board A for which IP address information was received was http://[redacted].com/xu5me9erdlpp/brochuer.rar.html.

To the extent the defendant and the court in *Reece* suggest that the issue of probable cause is dependent on having tied a particular individual to the illegal activity—as opposed to tying evidence of criminal activity to the place to be searched—that would be error. In a child pornography investigation, it *is the search and the subsequent forensics analysis that will answer the questions of whether the defendant actually downloaded the child pornography from the link*. As the court already understands, if these questions could be answered prior to any search, it would alleviate any need for the search. This court should set aside any such reasoning and apply Fourth Circuit precedent in determining that this search warrant was supported by probable cause.

B. PROBABLE CAUSE WAS NOT BASED ON STALE INFORMATION BECAUSE CHILD PORNOGRAPHY IS OFTEN STORED FOR LONG PERIODS OF TIME ON ELECTRONIC DEVICES.

Next, the defendant argues that the warrant is defective on staleness ground. The defendant's purported contention that the probable cause was based on stale information stems from the amount of time that lapsed between the date that someone in the defendant's residence clicked on the link (November 2, 2015) and the date of the search (April 12, 2016). *See* Def. Mot. to Suppress at 10. The argument is without merit.

It is true that "[a] valid search warrant may issue only upon allegations of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time. *United States* v. *McCall*, 740 F.2d 1331, 1335–36 (4th Cir. 1984). However, "the existence of probable cause cannot be determined by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit." *United States* v. *Richardson*, 607 F.3d 357, 370 (4th Cir. 2010). Instead, courts "look to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property seized." *McCall*, 740 F.2d at 1335.

Here, the facts and circumstances favor continued existence of probable cause. In the specific context of child pornography cases, like this one, the Fourth Circuit has recognized that "courts have concluded that a delay – even substantial delay – between distribution and the issuance of a search warrant does not render the underlying information stale." *Richardson,* 607 F.3d at 370. The reason is plain: "collectors and distributors of child pornography value their sexually explicit materials highly, rarely if ever dispose of such material, and store it for long periods in a secure place, typically their homes." *United States* v. *Lacy*, 119 F.3d 742, 746 (9th Cir. 1997).

Special Agent Eyler's affidavit in support of the search warrant established that just over five months (November 2, 2015–April 12, 2016) had elapsed between the time that someone from the defendant's residence clicked on the link and the search of that residence. This five-month gap is well within the time-frame as a matter of law to avoid any staleness issues. *See e.g.*, *United States* v. *Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) ("Information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned."); *United States* v. *Harvey*, 2 F.3d 1318, 1323 (3d. Cir. 1993) (holding that 15-month old information is not stale in child pornography context); *United States* v. *Frachette,* 583 F.3d 374, 378–79 (6th Cir. 2009) (information not stale where there was 18-month lapse between child pornography subscription and warrant to search defendant's home); *United States* v. *Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (three-year-old evidence of defendant's downloading of child pornography not stale).[3]

[3] *See also United States* v. *Riccardi*, 405 F.3d 852, 860-61 (10th Cir. 2005) (holding that information not stale where five-year old Kinko's receipt indicated defendant may have had a desire and ability to covert Polaroid photographs to digit format as is common among child pornographers); *United States* v. *Paull*, 551 F.3d 516, 522 (6th Cir. 2009) ("[B]ecause the crime [of child pornography] is generally carried out in the secrecy of the home and over a long period,

Though the defendant complains of the five-month gap, he cites not a single case finding such a warrant defective for staleness in the child pornography context.[4] Instead, the defendant attempts to distinguish this case from the wide and overwhelming body of law rejecting his staleness argument by claiming that the affidavit does not adequately establish that he is a collector of child pornography. As the defendant concedes, "[s]everal courts have rejected a Defendant's staleness argument in the event there are supporting facts included in an affidavit . . . supporting the notion that the individual subject to search was a "collector or distributor" of child pornography." Def's Mot. to Supp. at 11. There is no dispute that the affidavit contained the collector language which allowed the magistrate to conclude that child pornography was likely still at the premises. *See* affidavit at ¶¶ 21 - 26. So the defendant makes the only argument he can: that it was improper to include the collector language in the first place. In support, he relies on two inapposite cases: (1) *United States* v. *Richardson*; and (2) *United States* v. *Raymonda*. Neither case helps the defendant.

1. *United States* v. *Richardson* involved a child pornography investigation that originated from a tip from the National Center for Missing and Exploited Children regarding child pornography that was being trafficked using an email address that belonged to the defendant. 607 F.3d 357 (4th Cir. 2010). In *Richardson*, the defendant argued the warrant was stale because the

---

the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography.").

[4] The defendant does cite *United States* v. *Doyle*, which held that while "substantial amounts of time can elapse before probable cause to search for child pornography becomes stale," probable cause does not remain "ad infinitum." 650 F.3d 460, 475 (4th Cir. 2011). *Doyle* is factually inapposite from this defendant's case because in *Doyle* the affidavit did not specify when alleged child pornography was possessed. *Id.* at 469. Thus, "there was absolutely no indication in the affidavit as to when probable cause to search arose." *Id.* By contrast, Special Agent Eyler's affidavit contains a specific date and the time when a computer at the defendant's residence attempted to access the child pornography. *See* Affidavit at ¶¶ 16 and 18.

affidavit itself did not specify the date on which he possessed or emailed the illicit images. *Id.* at 369. The defendant argued that without the date, then anyone who *ever* possessed or distributed child pornography from the residence would be subject to search. *Id.* The Fourth Circuit rejected this argument and concluded that while the time is a "crucial element of probable cause," in the child pornography context "substantial delays" between the act and the issuance of the search warrant does not render it invalid. *Id.* at 370. This is because people who download and distribute child pornography tend to keep their collections for long periods of time.

Nothing in *Richardson* aids the defendant here. Unlike the affidavit in *Richardson*, the affidavit here *does* provide the date that someone attempted to download the child pornography, providing the magistrate with an exact date from which to evaluate whether the warrant was likely to contain a staleness defect. More to the point, nothing in *Richardson* can be read to undermine the use of the collector language in the present affidavit. Instead, the decision stresses that it is a "consensus" and "widespread view among the courts" that individuals who possess child pornography "value their sexually explicit materials highly," "rarely if ever dispose of such materials," and "store it for long periods in a secure place, typically in their homes." *Id.* Rather than help the defendant, *Richardson* effectively forecloses the very argument he attempts to make.

2. *United States* v. *Raymonda* is similarly of little help to the defendant. 780 F.3d 105 (2d Cir. 2015). In *Raymonda*, the Second Circuit held that a search warrant was based on stale information where the search took place nine-months after the defendant allegedly accessed child pornography from the website www.coolib.com. The court found that the warrant was based on stale information (though it refused to suppress the evidence under the good-faith exception) because the affidavit could not establish that defendant there was a collector of child pornography. *Raymonda*, however, noted that courts do find that a target can be a collector based on a "single

incident of possession" where the "suspect's access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files." *Id.* at 115.

Contrary to the defense's argument, such complicated steps do exist in the present matter. For example, in order to access the child pornography at issue in this case, a suspect likely had to download TOR, a browser that allows users to access the dark web, because Bulletin Board A is not available on the regular internet. Then, the suspect had to find his or her way to Bulletin Board A, a membership-based website with rules and administrators and dedicated to advertising child pornography in an organized manner. Then, the suspect had to navigate to a post containing thumbnails of child pornography. Then, the suspect had to click a link taking him or her to another website, enter a password, and download the files. At the time she sought the warrant, there was no reason for SA Eyler to believe that this particular child pornography file had been accessed any other way. This is sufficiently complicated to warrant inclusion of the collector language under the Second Circuit's decision in *Raymonda*.

This debate over Second Circuit case law, however, is mostly academic. Even if there were no complicated steps undertaken, the Second Circuit's analysis does not control here. And the Fourth Circuit has observed that, "information a year old is not stale as a matter of law in child pornography cases." *United States* v. *Davis*, 313 F. App'x 672, 674 (4th Cir. 2009) (citing *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005)). This forecloses the defendant's complaint that the warrant is defective on staleness grounds based on five-month-old information.

Further undermining the defendant's staleness argument is the information in the affidavit itself. A close read reveals that the language of the affidavit also accounts for the possibility that the defendant may not have collected the child pornography, and instead deleted it shortly after

acquiring it. *See* Affidavit at ¶ 23 ("Some of these individuals also have been found to . . . delete child pornography on their computers or digital devices on a cyclical or repetitive basis."). The affidavit notes that regardless of any such deleting behavior, however, forensic tools can still locate the evidence on the devices. *Id.* This is an important point because the only reason staleness would be an issue is if there were a reason to believe the evidence no longer existed at the premises. If the evidence is likely to be at the premises irrespective of whether the defendant collected or deleted the child pornography, the defendant's arguments about staleness would be rendered baseless.

As one court observed, "as child pornographers have become more tech savvy, so have law enforcement officers and prosecutors. With the assistance of forensic software, a skilled investigator can recover data from a computer that the user thought was deleted." *United States* v. *Moreland*, 665 F.3d 137, 142 (5th Cir. 2011). Judge Nachmanoff, when he signed the search warrant, also understood this basic fact because Special Agent Eyler included it in her affidavit. *See* Affidavit at ¶ 23 ("[E]vidence of such activity, included deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools."). Thus, whether the defendant collected or deleted his illicit material, the evidence was still likely to be at his residence, and thus, undermines any argument that agents waited too long to execute the search warrant at Bosyk's residence.

II. THE GOOD FAITH EXCEPTION APPLIES

Next, Bosyk argues that if the search warrant for his home was defective, the good faith exception, which would nonetheless permit the evidence to be admitted at trial, does not apply. This too is false. The good-faith exception clearly applies such that the evidence should not be suppressed even if the Court determines the affidavit lacks probable cause. *United States* v. *Leon*,

468 U.S. 897, 922 (1984).

Courts have held that even if a search warrant is ultimately found defective, the exclusionary rule is not always the proper remedy. *See e.g.*, *United State*s v. *Matish*, 193 F. Supp. 3d 585, 622 (E.D. Va. June 23, 2016) (holding that "even if there existed defects in the warrant or issuance, the Court finds that suppression would still be inappropriate under the good faith exception to the exclusionary rule."). Notably, suppression is a remedy of last resort. *Hudson* v. *Michigan*, 547 U.S. 586, 591 (2006). More importantly, the exclusionary remedy has been "restricted to those areas where its remedial objectives are thought most efficaciously served." *United States* v. *Calandra*, 414 U.S. 338, 348 (1974). As a result, suppression only applies where it would "result in appreciable deterrence." *Leon*, 468 U.S. at 909.

The deterrence that the courts look to is deterrence against police misconduct. Given the social costs extracted by the exclusionary rule, the police conduct warranting suppression must be "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring* v. *United States*, 555 U.S. 135, 144 (2009). Thus, only police conduct that is deliberate misconduct, reckless, or grossly negligent will support the application of the exclusionary rule. Where police act with "objective good faith" that their conduct was legal, exclusion is prohibited. *Leon*, 468 U.S. at 920.

Bosyk points to no instance of agent misconduct that would warrant deterrence in this case. The most Bosyk can muster on this point is arguing that the affidavit is *too truthful*. For example, he faults the affidavit for failing to claim that Bosyk "utilized a password or tried to use a password in attempting to access the subject video." Def. Mot to Suppress. at 13. Further, he claims that is was wrong for the affidavit not to include language that "the URL was accessed by the IP address via Bulletin Board A" and that the affidavit spends too much time educating the judge on Bulletin

Board A. *Id.* at 14. Finally, he reasserts his protest, already addressed above, that it was inappropriate to include the collector language. *Id.* at 13. Based on these claims, the defendant argues that Judge Nachmanoff was misled and that the affidavit itself was so lacking in indicia of probable cause to render official belief in its existence unreasonable, and compels this court to order a hearing under *United States* v. *Franks*.[5] *See* Def's Mot. to Suppress. at 15-16.

A. A FRANKS HEARING IS UNWARRANTED

A defendant "is generally not entitled to challenge the veracity of a facially valid search warrant affidavit." *United States* v. *Allen*, 631 F.3d 164, 171 (4th Cir. 2011) (rejecting defendant's request for evidentiary hearing to challenge search warrant). However, in *Franks* v. *Delaware*, the Supreme Court carved out a narrow exception where the defendant can receive an evidentiary hearing if he makes a substantially preliminary showing that false statements in the affidavit were "knowingly or recklessly included in an affidavit . . . *and* that, without those statements the affidavit cannot support a probable cause finding." *Id.* (emphasis in original). In order to make the "rigorous" showing necessary for a *Franks* hearing, the showing must be "more than conclusory and should include affidavits or other evidence to overcome the presumption of [the warrant's validity]." *United States* v. *Clenney*, 631 F.3d 658, 663 (4th Cir. 2011).

Where a defendant argues that an agent "omitted several facts from the warrant affidavit[], the Franks threshold is even higher." *Id.* at 664; *accord United States* v. *Tate*, 524 F.3d 449, 454–55 (4th Cir. 2008). The defendant must demonstrate that he omissions were "designed to mislead, . . . or made in reckless disregard of whether they would mislead." *United States* v. *Colkley*, 899 F.3d 297, 301 (4th Cir. 1990). Finally, even if that showing is made, a *Franks* hearing is

[5] The United States addressed the probable cause arguments in Section I of this memorandum. Consequently, the United States will focus only on the claim that Judge Nachmanoff was mislead in this section, but does not, in any way, concede that the search warrant was lacking for probable cause.

unwarranted unless the defendant can show that "the omissions were material, meaning that their inclusion in the affidavit would defeat probable cause." *Id.*

The defendant does not and cannot meet this burden. So to convince this court that there is an issue in this case where there is none, the defendant again clutches to *Reece*. The court in *Reece* found that it was misleading for the agent omit that: (1) there was no present evidence that the defendant was a member of Bulletin Board A; (2) that there was no present evidence that the defendant entered the password after clicking the link; and (3) that there was no evidence that the defendant was a collector.[6]

With all due respect to the court in *Reece*, it is exceedingly unlikely that Judge Nachmanoff was misled by the absence of disclaimers. If law enforcement had evidence that Bosyk (or someone at his residence) actually was a member of Bulletin Board A or that he definitively entered the password, they would have included it in the affidavit to support probable cause. They did not have that evidence at the time and therefore did not include those statements. There is no requirement that disclaimers be included where the affidavit is entirely truthful. And the affidavit noted that it included only those facts necessary for probable cause and not all information known about the investigation. Affidavit at ¶ 4.

It is not surprising that Judge Nachmanoff approved the search warrant despite there being no direct evidence that the defendant was a member of Bulletin Board A and despite the fact that the agents could not definitively determine whether the defendant entered the password. That

[6] There was circumstantial evidence that whoever clicked the link was a member of Bulletin Board A: 1) the link was clicked the same day it was posted on Bulletin Board A, and 2) law enforcement had no reason to believe at the time that this child-pornography link originated anywhere other than Bulletin Board A. Further, there was also no evidence that he was *not* a member of Bulletin Board A. The affidavit made clear that the focus was on individuals who clicked on a link containing child pornography which originated at Bulletin Board A.

information was not necessary for the probable cause determination. The undisputed facts are that: (1) A link containing child pornography appeared on Bulletin Board A; (2) less than 24 hours after the link was posted on Bulletin Board A, someone at the defendant's residence clicked on that link. As the court in *Evans* made clear, these two facts in conjunction with each other allow a reasonable magistrate to conclude that the person at the defendant's residence visited Bulletin Board A and clicked on the link at Bulletin Board A (and, therefore, saw the posting, the child pornography thumbnails therein, and understood that the link contained child pornography). *See United States* v. *Evans*, 5:16-cr-20292, Doc. No. 69, at 14.

Further, the facts in this case readily distinguish it from *Reece*. *Reece* found suppression warranted in large part because it found the multiple errors related to the affidavit and the agent's testimony, evincing a reckless disregard for accuracy. *Reece*, 2:14-cr-104, Doc. No. 44 at 20. This included a statement in the affidavit that the subject of the affidavit had traded child pornography via an "email account," when it was actually an IP address at issue. *Id.* at 19. And the agent testified that he apparently had not even reviewed that paragraph in the affidavit. *Id.* at 19–20. There were also inconsistencies in the agent's testimony about whether he applied for a no-knock warrant and the number of other leads he had received related to the defendant. *Id.* at 22–23. The affidavit at issue here does not contain the type or number of errors found significant in the *Reece* case.

Putting aside the fact that the affidavit in this case as written is not misleading, there is a larger problem with the defendant's request for a *Franks* hearing. It ignores the law. The Fourth Circuit has made clear that it is not enough that an omission "may have affected the outcome of the probable cause determination." *Colkley*, 899 F.2d. at 301 (4th Cir. 1990). Instead, "to be material under *Franks*, an omission must be necessary to the finding of probable cause." *Id.*

(quoting *Franks*, 438 U.S. at 156). In fact, "for an omission to serve as the basis for a hearing under Franks, it must be such that its inclusion in the affidavit would defeat probable cause . . . ." *Id.* "Omitted information that is potentially relevant but not dispositive is not enough to warrant a Franks hearing." *Id.* The allegedly omitted information in this case was not dispositive to probable cause, so the defendant's argument for a *Franks* hearing must fail.

This very court has recognized the importance of this Fourth Circuit precedent when it recently noted that "invalidating warrants for omissions potentially opens officers to endless conjecture about the investigative leads, fragments of information or other matters that might, if included, have redounded to the defendant's benefit." *United States* v. *Young*, 260 F. Supp. 3d 530 (E.D. Va, May 9, 2017) (Brinkema, J.). The danger in the court's view was clear: "[t]he potential for endless rounds of *Franks* hearings to contest facially sufficient warrants is readily apparent." *Id.*

This court's warning was indeed clairvoyant because it was the decision in *Reece* which led this defendant to request a *Franks* hearing to contest a facially sufficient warrant. But in the end, the warrant here was based on probable cause. The only question Judge Nachmanoff had to consider was whether there was a "fair probability" that child pornography would be at Bosyk's residence. That is it. Whether Bosyk was a member or Bulletin Board A is immaterial to that determination. Furthermore, the fact that there was no evidence that Bosyk entered the password does not undermine probable cause because probable cause would only be defeated if there was definitive proof that Bosyk (or someone at his residence) *had not* entered the password. While including these details might have been "potentially relevant," they were not dispositive. Thus, neither, as the defendant calls them, "omission" justify a *Franks* hearing.

Nor does the affidavit's inclusion of information about Bulletin Board A or the inclusion of collector language render it misleading. Simply put, the information about Bulletin Board A was included because that was the basis for the entire investigation into the child-pornography file at issue. Likewise, there was strong circumstantial evidence that Bulletin Board A was where the pornography was downloaded given that law enforcement had no knowledge the child pornography link in question had been posted anywhere else. As the affidavit makes clear, someone at the defendant's residence attempted to download the child pornography within 24 hours of it being posted on Bulletin Board A. Affidavit at ¶ 16. Unsurprisingly, the defendant completely ignores this crucial fact in his memorandum. But it is for that reason—that there was a fair probability that the individual who downloaded this material received it from Bulletin Board A—that the collector language is appropriate. A person who visits and downloads child pornography from a website like Bulletin Board A is properly classified as a collector. This court should, therefore, resist calls for a *Franks* hearing on the basis of these inclusions in the affidavit.

Finally, The defendant's argument for a *Franks* hearing fails for yet another reason: the defendant has failed to make the requisite showing justifying the need for the hearing. To make this showing the burden is squarely on the defendant to prove it through "affidavits or statements of witnesses" demonstrating the falsity of the affidavit. *See Davis*, 313 F. App'x at 673. The Fourth Circuit has cautioned that the "burden of making the necessary showing is thus a heavy one to bear." *United States* v. *Tate*, 524 F.3d 449, 454 (4th Cir. 2008). The defendant has not even attempted to meet this burden (he has filed no affidavits or presented any evidence), and so his request for a *Franks* hearing must be denied.

B. GOOD FAITH EXISTS WHERE THE AGENT RELIES ON THE PROBABLE CAUSE DETERMINATION OF THE MAGISTRATE

Having failed to establish that there are any material omissions in the affidavit or that the inclusion of information about Bulletin Board A or the collector language was misleading, the defendant must now contend with the undisputed law on the good faith exception. Simply, where, as is the case here, an agent relies on the determination of a magistrate judge to execute a search warrant, the good-faith exception applies. As the Supreme Court has observed, "[u]sually a warrant issued by a magistrate . . . suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *United States* v. *Leon*, 468 U.S. 897, 922 (1984). Here Magistrate Judge Nachmanoff issued the warrant only after he found probable cause for the search. Law enforcement relied on that determination. Consequently, this case falls squarely under the protection of the good-faith exception and provides yet another reason to deny the defendant's motion.

CONCLUSION

For the aforementioned reasons, the United States respectfully requests that the court deny the defendant's motion to suppress the evidence in this case.

Date: January 17, 2018

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s

Nathaniel Smith III
Assistant U.S. Attorney
Lauren Britsch
Special Assistant U.S. Attorney (LT)
U.S. Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Ph: (703) 299-3700

CERTIFICATE OF SERVICE

I hereby certify that on January 17, 2018, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will automatically send electronic notification of such filed (NEF) to the following:

Mark B. Williams
Mark B. Williams & Associates, PLC
27 Culpepper Street
Warrenton, Virginia 20186
(540)347-6595
mbwilliams@mbwalaw.com

Counsel for Nikolai Bosyk

By: /s
Nathaniel Smith III
Assistant U.S. Attorney
U.S. Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Ph: (703) 299-3700
Nathaniel.Smith2@usdoj.gov